EP00/05642

PCT/EP 00 / 05642

KONINKRIJK DER NEDERLANDEN

10/018605

Bureau voor de Industriële Eigendom

REC'D 21 JUL 2000
WIPO PCT

Hierbij wordt verklaard, dat in Nederland op 25 juni 1999 onder nummer 1012435,

ten name van:

KONINKLIJKE KPN N.V.

te Groningen

een aanvrage om octrooi werd ingediend voor:

"Systeem voor beveiligde opslag en beheer in een TTP server",

en dat de hieraan gehechte stukken overeenstemmen met de oorspronkelijk ingediende stukken.

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

Rijswijk, 29 mei 2000.

De Directeur van het Bureau voor de Industriële Eigendom,
voor deze,

P.J.C. van den Nieuwenhuijsen.

UITTREKSEL

Systeem voor beveiligde opslag in een TTP server. Een bestand (Txt) wordt van een eerste (A) naar een tweede gebruiker (B) verzonden na vercijfering met een sessiesleutel (SesKey), welke vercijferd wordt met de publieke sleutel (PubKeyB) van de tweede gebruiker. De sessiesleutel (SesKey) wordt door de eerste gebruiker tevens vercijferd met de publieke sleutel (PubKeyTTP) van de TTP server, die na ontvangst die sessiesleutel ontcijfert met zijn private sleutel (SecKeyTTP). De TTP server vercijfert vervolgens de sessiesleutel (SesKey) en de (oorspronkelijke) publieke sleutel (PubKeyA) van de eerste gebruiker (A) met een "publieke" een opslagsleutel (PubStorKey); de vercijferde sessiesleutel ((SesKey)PubStorKey) en publieke sleutel ((PubKeyA)PubStorKey) van de eerste gebruiker worden tezamen met het vercijferde bestand ((Txt)SesKey) in een opslagmedium (DB) opgeslagen. Ze zijn door de TTP herwinbaar door ontcijfering met de private opslagsleutel (SecStorKey) en kunnen, vercijferd met de actuele publieke sleutels (PubKeyA' resp. PubKeyB') van de gebruikers, worden overgedragen.

(Fig. 1)

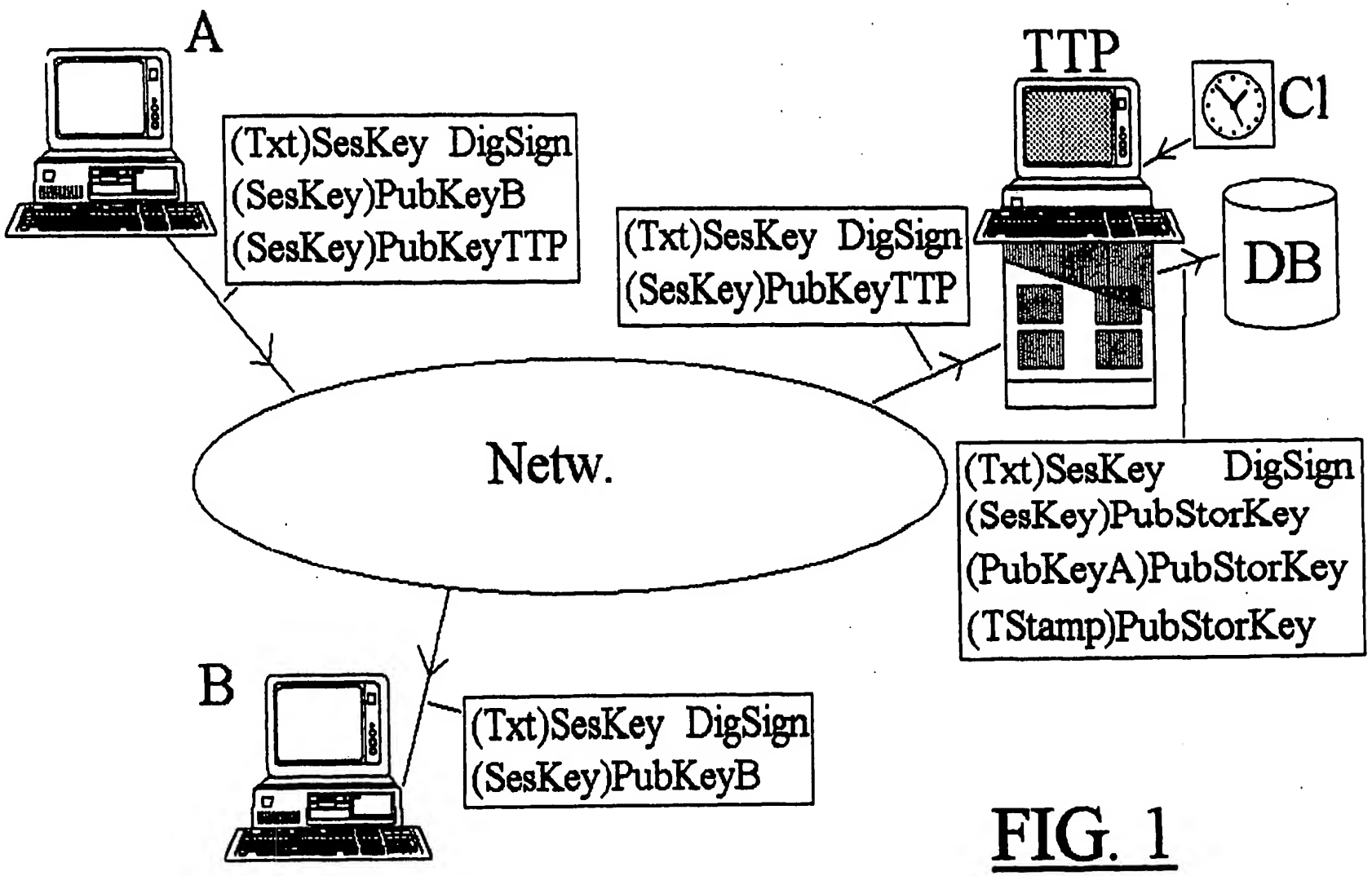
A
(Txt)SesKey DigSign
(SesKey)PubKeyB
(SesKey)PubKeyTTP
TTP
Cl
DB
(Txt)SesKey DigSign
(SesKey)PubKeyTTP
Netw.
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
B
(Txt)SesKey DigSign
(SesKey)PubKeyB

FIG. 1

Systeem voor beveiligde opslag en beheer in een TTP server

ACHTERGROND VAN DE UITVINDING

De uitvinding heeft betrekking op een systeem voor beveiligde opslag en beheer in een TTP server, van copieën van digitale bestanden die via een transmissiekanaal van een eerste naar een tweede gebruiker worden gezonden.

De uitvinding betreft, met andere woorden, een tijdloos sleutel- & opslagsysteem voor ten behoeve van het op een veilige manier langdurig opslaan van electronisch uitgewisselde (digitaal beveiligde) informatie en het beveiligd beschikbaar stellen (secure retrieval) van de opgeslagen data.

De weinige bekende systemen hebben de volgende nadelen:

1) Huidige beveiligingstechnieken kennen een beperkte kraakbaarheidsduurgarantie.

2) Beperkte beveiligingsgaranties voor tijdens en na langdurige opslag.

3) Veel opslagruimte en inspanning nodig voor sleutelbeheer.

4) Beveiligde langdurige opslag en het daarbij behorende sleutel- en opslagbeheer is nu of niet geregeld of zeer complex van opzet.

5) Door de steeds veranderende soft- en hardware is het zeer moeilijk om electronische tijdloosheid te garanderen.

B. SAMENVATTING VAN DE UITVINDING

De uitvinding beoogt de genoemde nadelen te ondervangen. Daartoe voorziet de uitvinding in een systeem met middelen voor het uitvoeren van de functionaliteiten: "Secure Archiving", "Re-encryption", "Secure Retrieval", welke hieronder zullen worden besproken. Afzonderlijk worden daarbij de optionele items "Digital Sign" en "Timestamp" behandeld.

"Secure Archiving"

Als een bestand, volgens de huidige stand van de techniek, op veilige wijze van een eerste gebruiker naar een tweede gebruiker wordt verzonden, wordt het bestand vercijferd met een symmetrische sessiesleutel, die op zijn beurt wordt vercijferd met de publieke sleutel van de tweede gebruiker. Die tweede gebruiker kan de sessiesleutel ontcijferen met zijn private sleutel en het bestand zelf met de aldus ontcijferde sessiesleutel.

8 II

Volgens de uitvinding wordt de sessiesleutel door de eerste gebruiker tevens vercijferd met de publieke sleutel van een "in-line" (d.w.z. opgenomen in het transmissiekanaal tussen de eerste en tweede gebruiker) TTP server, welke TTP server de ontvangen sessiesleutel ontcijfert met zijn private sleutel. Daarna vercijfert de TTP server de ontcijferde sessiesleutel met een "publieke" opslagsleutel. De met die publieke opslagsleutel vercijferde sessiesleutel en het met de sessiesleutel vercijferde bestand worden vervolgens in een opslagmedium van de TTP opgeslagen.

Opgemerkt wordt dat hierboven en hieronder wordt gesproken van publieke en private sleutels. Deze zijn van algemene bekendheid. In het algemeen vormen een publieke en een private sleutel een asymmetrisch sleutelpaar. Als een bestand of een code met de publieke sleutel van een asymmetrisch sleutelpaar vercijferd is, kan dat bestand of die code alleen worden ontcijferd met behulp van de bijhorende private sleutel en vice versa. In het algemeen zijn de publieke sleutels voor "het publiek" beschikbaar, bijvoorbeeld via een openbaar toegankelijke database zoals www.pgp.com. In de onderhavige aanvrage wordt er van uitgegaan dat de gebruikers en de TTP elk over een sleutelpaar beschikken, elk bestaande uit een publieke en een private sleutel en in het bijzonder bedoeld voor beveiliging van de onderlinge data-uitwisseling van de bestanden en codes. De TTP beschikt daarenboven over een sleutelpaar dat uitsluitend binnen de TTP wordt gebruikt; de "publieke" en de private sleutel dienen voor beveiligde opslag respectievelijk herwinning ("secure retrieval") van bestanden en codes. De publieke opslagsleutel wordt niet, zoals normaliter bij publieke sleutels het geval is, publiekelijk ter beschikking gesteld.

"Re-encryption"

Bij wijze van "periodiek onderhoud" -uit veiligheidsoverwegingen- kan de TTP server op gezette tijden het bestand opnieuw in het opslagmedium opslaan. Daartoe wordt eerst de sessiesleutel, waarmee het bestand is vercijferd, herwonnen, door ontcijfering -met de private opslagsleutel- van de opgeslagen (vercijferde) sessiesleutel Vervolgens wordt het in het opslagmedium opgeslagen vercijferde bestand met de herwonnen sessiesleutel ontcijferd.

De TTP server genereert vervolgens een nieuw asymmetrisch opslagsleutel-paar, bestaande uit een nieuwe publieke opslagsleutel (die buiten de TTP niet beschikbaar wordt gesteld) en een nieuwe private opslagsleutel, en een nieuwe versie van de symmetrische sessiesleutel, waarna de TTP het ontcijferde bestand met de nieuwe sessiesleutel vercijfert en in het opslagmedium opslaat.

De TTP vercijfert tevens de nieuwe sessiesleutel met de nieuwe publieke opslagsleutel en slaat die vercijferde sessiesleutel in het opslagmedium op.

"Secure Retrieval"

Voor beveiligde terugwinning van het opgeslagen bestand en overdracht ervan naar de eerste en/of tweede gebruiker, wordt de symmetrische sessiesleutel herwonnen uit het opslagmedium door ontcijfering, met de private opslagsleutel, van de opgeslagen vercijferde sessiesleutel. De herwonnen sessiesleutel wordt vervolgens vercijferd met de actuele publieke sleutel van de eerste resp. tweede gebruiker en via het transmissiekanaal naar die gebruiker overgedragen, tezamen met een copie van het in het opslagmedium opgeslagen, met de sessiesleutel vercijferde bestand. De gebruiker kan na ontvangst van de vercijferde sessiesleutel, de sessiesleutel daaruit herwinnen door ontcijfering met zijn private sleutel. Vervolgens kan de gebruiker het met de sessiesleutel vercijferde bestand ontcijferen met behulp van de herwonnen sessiesleutel.

"Digital Sign"

De publieke sleutel van de eerste gebruiker kan -zoals bekend- worden gebruikt ter verificatie van een digitale handtekening van het bestand. Een probleem doet zich voor als -wat vaak voorkomt- de eerste gebruiker op zeker moment, nadat het bestand in de TTP server is opgeslagen, een nieuw sleutelpaar (omvattende een publieke en een private sleutel) genereert en het oude laat vervallen. Om die reden is het van belang de (oorspronkelijke) publieke sleutel van de eerste gebruiker in de TTP server op te slaan, daar alleen die oorspronkelijke sleutel gebruikt kan worden voor verificatie van de digitale handtekening van het opgeslagen, later opvraagbare bestand.

Voor dat geval vercijfert de TTP server, na ontvangst van het vercijferde bestand tevens de -op dat moment publiek beschikbare- publieke sleutel van de eerste gebruiker, met de publieke opslagsleutel, en slaat die vercijferde publieke sleutel in het opslagmedium op.

Periodiek -als "periodiek onderhoud"- ontcijfert de TTP server de in het opslagmedium opgeslagen vercijferde (oorpsronkelijke) publieke sleutel van de eerste gebruiker met de private opslagsleutel, en vercijfert de ontcijferde publieke sleutel van de eerste gebruiker met de nieuw gegenereerde publieke opslagsleutel en slaat die opnieuw vercijferde sleutel in het opslagmedium op.

De publieke sleutel van de eerste gebruiker kan -bij opvraging van het opgeslagen bestand- uit het opslagmedium worden herwonnen door ontcijfering met de private opslagsleutel, van die opgeslagen sleutel. De aldus herwonnen publieke sleutel van de eerste gebruiker wordt vervolgens vercijferd met de -op dat moment publiek beschikbare- publieke sleutel van de opvragende eerste of tweede gebruiker en via het transmissiekanaal overgedragen. De gebruiker kan, na ontvangst van die vercijferde publieke sleutel de oorspronkelijke publieke sleutel van de eerste gebruiker herwinnen door ontcijfering met zijn actuele private sleutel; vervolgens kan de digitale handtekening van het herwonnen bestand met behulp van de herwonnen oorspronkelijke publieke sleutel van de eerste gebruiker worden geverifieerd.

"Timestamp"

De TTP server kan desgewenst, na ontvangst en opslag van het vercijferde bestand een tijdcode genereren en die, gelinkt aan het opgeslagen bestand en vercijferd met de publieke opslagsleutel, in het opslagmedium opslaan. Bij opvraging van het opgeslagen bestand door de eerste of tweede gebruiker, wordt de tijdcode ontcijferd en vervolgens vercijferd met voor die gebruiker actuele publieke sleutel en naar de gebruiker overgedragen. De gebruiker kan de vercijferde tijdcode ontcijferen met zijn actuele private sleutel.

FIGUURBESCHRIJVING

De uitvinding wordt hierna aan de hand van een aantal figuren nader geïllustreerd. De figuren 1, 2 en 3 illustreren respectievelijk de functies “Secure Archiving”, "Re-encryption", "Secure Retrieval", incl. de items "Digital Sign" en de "Timestamp".

Figuur 1: “Secure Archiving”

Een bestand **Txt** wordt van een eerste gebruiker **A** naar een tweede gebruiker **B** verzonden na te zijn vercijferd met een symmetrische sessiesleutel **SesKey**. Die

sessiesleutel wordt vercijferd met de publieke sleutel **PubKeyB** van de tweede gebruiker. Die kan de sessiesleutel ontcijferen met zijn private sleutel **SecKeyB** en het bestand zelf met de ontcijferde sessiesleutel.

De sessiesleutel wordt door de eerste gebruiker tevens vercijferd met de publieke sleutel van de TTP server **PubKeyTTP**, die na ontvangst die sessiesleutel ontcijfert met zijn private sleutel **SecKeyTTP**. Daarna vercijfert de TTP server de ontcijferde sessiesleutel met een "publieke" opslagsleutel **PubStorKey** van de TTP.

De (transmissie)sleutels van de gebruikers A en B vormen elk een asymmetrisch sleutelpaar, **KeyPairA** resp. **KeyPairB**, bestaande uit **PubKeyA** en **SecKeyA**, resp. **PubKeyB** en **SecKeyB**. De TTP gebruikt een het sleutelpaar **KeyPairTTP**, bestaande uit **PubKeyTTP** en **SecKeyTTP**. Tenslotte gebruikt de TTP voor de beveiligde opslag een asymmetrisch sleutelpaar **StorKeyPair**, bestaande uit de sleutels **PubStorKey** en **SecStorKey**; in tegenstelling tot de voorgaande publieke sleutels, is **PubStorKey**, evenals **SecStorKey**, niet publiek beschibaar, maar wordt uitsluitend binnen de TTP gebruikt.

De met de publieke opslagsleutel **PubStorKey** vercijferde sessiesleutel **(SesKey)PubStorKey** en het met de sessiesleutel **SesKey** vercijferde bestand **(Txt)SesKey** worden vervolgens in een opslagmedium **DB** van de TTP opgeslagen.

"Digital Sign"

De publieke sleutel **PubKeyA** van de eerste gebruiker **A** kan worden gebruikt ter verificatie van een digitale handtekening **DigSign** van het bestand **Txt**. In dat geval vercijfert de TTP server, na ontvangst van het vercijferde bestand **(Txt)SesKey** tevens de -op dat moment publiek beschikbare- publieke sleutel **PubKeyA** van de eerste gebruiker **A**, met de publieke opslagsleutel **PubStorKey**, en slaat die vercijferde publieke sleutel **(PubKeyA)PubStorKey** in het opslagmedium **DB** op.

"Timestamp"

De TTP server kan, na ontvangst en opslag van het vercijferde bestand **(Txt)SesKey** een tijdcode **TStamp** genereren en die, na vercijfering met de publieke opslagsleutel **PubStorKey** en gelinkt aan het opgeslagen bestand, als **(TStamp)PubStorKey** in het opslagmedium **DB** opslaan.

Figuur 2: "Re-encryption"

Als "periodiek onderhoud" ontcijfert de TTP server het in het opslagmedium opgeslagen vercijferde bestand **(Txt)SesKey** met de sessiesleutel **SesKey**, die daartoe door ontcijfering van de opgeslagen sessiesleutel **(SesKey)PubStorKey** met de private opslagsleutel **SecStorKey**, wordt herwonnen. De TTP server genereert vervolgens een nieuw opslagsleutelpaar **StorKeyPair**, omvattende een nieuwe "publieke" opslagsleutel **PubStorKey'** en een nieuwe private opslagsleutel **SecStorKey'**, alsmede een nieuwe versie van de symmetrische sessiekey **SesKey'**. De TTP vercijfert vervolgens het ontcijferde bestand **Txt** met de nieuwe sessiesleutel **SesKey'** en slaat het aldus vercijferde bestand **(Txt)SesKey'** in het opslagmedium DB op.

De TTP vercijfert tevens de nieuwe sessiesleutel met de nieuwe publieke opslagsleutel **PubStorKey'** en slaat de aldus vercijferde sessiesleutel **(SesKey')PubStorKey'** in het opslagmedium DB op.

"Digital Sign"

Bij het periodieke onderhoud ontcijfert de TTP server ook de in het opslagmedium opgeslagen vercijferde publieke sleutel **(PubKeyA)PubStorKey** van de eerste gebruiker met de private opslagsleutel **SecStorKey**, en vercijfert vervolgens de ontcijferde publieke sleutel **PubKeyA** met de nieuw gegenereerde publieke opslagsleutel **PubStorKey'** en slaat de aldus vercijferde publieke sleutel **(PubKeyA)PubStorKey'**in het opslagmedium op.

"Timestamp"

Bij het periodieke onderhoud ontcijfert de TTP server ook de in het opslagmedium opgeslagen vercijferde tijdcode **(TStamp)PubStorKey** met de private opslagsleutel **SecStorKey**, en vercijfert vervolgens de ontcijferde tijdcode **TStamp** met de nieuw gegenereerde publieke opslagsleutel **PubStorKey'** en slaat de aldus vercijferde tijdcode **(TStamp)PubStorKey'**in het opslagmedium op.

Figuur 3: "Secure Retrieval"

Voor beveiligde herwinning van het bestand **Txt** en overdracht ervan naar de eerste resp. tweede gebruiker **A** resp. **B**, wordt de symmetrische sessiesleutel **SesKey** herwonnen uit het opslagmedium door ontcijfering, met de private opslagsleutel **SecStorKey**, van de

opgeslagen, vercijferde sessiesleutel **(SesKey)PubStorKey**. De herwonnen sessiesleutel **SesKey** wordt vervolgens vercijferd met de dan actuele publieke sleutel **PubKeyA'** resp. **PubKeyB'** van de opvragende eerste resp. tweede gebruiker **A** resp. **B** en via het transmissiekanaal naar die gebruiker overgedragen, tezamen met een copie van het in het opslagmedium opgeslagen bestand, waarbij de gebruiker, na ontvangst van de vercijferde sessiesleutel **(SesKey)PubKeyA'** resp. **(SesKey)PubKeyB'**, de sessiesleutel daaruit kan herwinnen door ontcijfering met zijn private sleutel **SecKeyA'** resp. **SecKeyB'**, en vervolgens het met de sessiesleutel vercijferde bestand **(Txt)SesKey** kan ontcijferen met behulp van de herwonnen sessiesleutel.

"Digital Sign"

De voor verificatie van de digitale handtekening van het herwonnen bestand noodzakelijke oorspronkelijke publieke sleutel **PubKeyA** van de eerste gebruiker kan worden herwonnen uit het opslagmedium door ontcijfering, met de private opslagsleutel **SecStorKey**, van de opgeslagen, met de publieke opslagsleutel vercijferde, publieke sleutel **(PubKeyA)PubStorKey** van de eerste gebruiker. De aldus herwonnen, ontcijferde publieke sleutel **PubKeyA** van de eerste gebruiker wordt vervolgens vercijferd met de actuele publieke sleutel **PubKeyA'** resp. **PubKeyB'** van de opvragende eerste resp. tweede gebruiker **A** resp. **B** en via het transmissiekanaal naar de gebruiker overgedragen. De gebruiker kan, na ontvangst van die vercijferde publieke sleutel **(PubKeyA)PubKeyA'** resp. **(PubKeyA)PubKeyB'** de oorspronkelijke publieke sleutel **PubKeyA** van de eerste gebruiker daaruit herwinnen door ontcijfering met zijn actuele private sleutel **SecKeyA'** resp. **SecKeyB'**; vervolgens kan de digitale handtekening **DigSign** van het bestand **Txt** met behulp van de herwonnen publieke sleutel **PubKeyA** van de eerste gebruiker worden geverifieerd.

Opgemerkt wordt dat het voorkeur geniet om -anders dan in figuur 3 is weergegeven- de digitale handtekening **DigSign** niet onvercijferd naar de eerste resp. tweede gebruiker te verzenden, maar vercijferd met de publieke sleutel van gebruiker **A** resp. **B**: in plaats van "**DigSign**" zendt de TTP server dan "**(DigSign)PubKeyA'**" resp. "**(DigSign)PubKeyB'**". Aan gebruikerszijde kan de digitale handtekening worden

herwonnen door ontcijfering met de private sleutels van **A** en **B**, **SecKeyA** resp. **SecKeyB**.

"Timestamp"

Bij opvraging van het opgeslagen bestand door de eerste of tweede gebruiker, wordt de tijdcode eerst herwonnen door ontcijfering van **(TStamp)PubStorKey** met de private opslagsleutel **SecStorKey.** De herwonnen tijdcode wordt vervolgens vercijferd met des gebruiker's actuele publieke sleutel **PubKeyA'** resp. **PubKeyB'** en naar die gebruiker overgedragen. Daarna kan de gebruiker de vercijferde tijdcode **(TStamp)PubKeyA'** resp. **(TStamp)PubKeyB'** ontcijferen met zijn actuele private sleutel **SecKeyA'** resp. **SecKeyB'**.

CONCLUSIES

1. Systeem voor beveiligde opslag en beheer in een TTP server, van copieën van digitale bestanden die via een transmissiekanaal van een eerste naar een tweede gebruiker worden gezonden, **MET HET KENMERK DAT**

een bestand (Txt) van de eerste gebruiker (A) naar een tweede gebruiker (B) wordt verzonden na te zijn vercijferd met een symmetrische sessiesleutel (SesKey), welke sessiesleutel vercijferd wordt met behulp van de publieke sleutel (PubKeyB) van een eerste a-symmetrisch sleutelpaar (KeyPairB), behorend bij de tweede gebruiker, welke tweede gebruiker na ontvangst de sessiesleutel kan ontcijferen met behulp van de private sleutel (SecKeyB) van dat eerste a-symmetrische sleutelpaar (KeyPairB) en vervolgens het bestand kan ontcijferen met behulp van de aldus ontcijferde sessiesleutel,

waarbij de sessiesleutel (SesKey) door de eerste gebruiker (A) tevens vercijferd wordt met behulp van de publieke sleutel (PubKeyTTP) van een tweede a-symmetrisch sleutelpaar (KeyPairTTP), behorend bij de TTP server, welke TTP server na ontvangst die sessiesleutel ontcijfert met behulp van de private sleutel (SecKeyTTP) van dat tweede a-symmetrische sleutelpaar (KeyPairTTP), waarna de TTP server de ontcijferde sessiesleutel (SesKey) vercijfert met behulp van de publieke sleutel van een derde a-symmetrisch sleutelpaar (StorKeyPair), hierna publieke opslagsleutel (PubStorKey) genoemd, en de met die publieke opslagsleutel vercijferde sessiesleutel ((SesKey)PubStorKey), tezamen met het met de sessiesleutel (SesKey) vercijferde bestand ((Txt)SesKey), in een opslagmedium (DB) opslaat.

2. Systeem volgens conclusie 1, **MET HET KENMERK DAT**, periodiek,

de TTP server het in het opslagmedium opgeslagen vercijferde bestand ((Txt)SesKey) ontcijfert met de sessiesleutel (SesKey), die daartoe tevoren wordt herwonnen door ontcijfering van de opgeslagen vercijferde sessiesleutel ((SesKey)PubStorKey) met de private sleutel van het derde sleutelpaar (StorKeyPair), hierna private opslagsleutel (SecStorKey) genoemd;

de TTP server vervolgens een nieuwe versie van het derde sleutelpaar genereert, omvattende een nieuwe publieke opslagsleutel (PubStorKey') en een nieuwe private opslagsleutel (SecStorKey'), en een nieuwe versie van de symmetrische sessiekey

(SesKey'), waarna de TTP het ontcijferde bestand (Txt) vercijfert met de nieuwe sessiesleutel (SesKey') en het aldus vercijferde bestand ((Txt)SesKey') in het opslagmedium (DB) opslaat;
de TTP server de nieuwe sessiesleutel (SesKey') vercijfert met de nieuwe publieke opslagsleutel (PubStorKey') en de aldus vercijferde sessiesleutel ((SesKey')PubStorKey') in het opslagmedium (DB) opslaat.

3. Systeem volgens conclusie 1, **MET HET KENMERK DAT** voor beveiligde herwinning van het bestand (Txt) en overdracht ervan naar de eerste gebruiker (A) resp. tweede gebruiker (B) de symmetrische sessiesleutel (SesKey) uit het opslagmedium wordt herwonnen door ontcijfering, met de private opslagsleutel (SecStorKey), van de opgeslagen vercijferde sessiesleutel ((SesKey)PubStorKey), waarna de herwonnen sessiesleutel (SesKey) vervolgens wordt vercijferd met de actuele publieke sleutel (PubKeyA' resp. PubKeyB') van de eerste resp. tweede gebruiker (A resp. B) en via het transmissiekanaal naar de gebruiker wordt overgedragen, tezamen met een copie van het in het opslagmedium opgeslagen bestand ((Txt)SesKey), waarbij de gebruiker, na ontvangst van de vercijferde sessiesleutel ((SesKey)PubKeyA' resp. (SesKey)PubKeyB'), de sessiesleutel daaruit kan herwinnen door ontcijfering met des gebruiker's private sleutel (SecKeyA' resp. SecKeyB'), en vervolgens het vercijferde bestand ((Txt)SesKey) kan ontcijferen met behulp van de herwonnen sessiesleutel.

4. Systeem volgens conclusie 1, waarbij de publieke sleutel (PubKeyA) van de eerste gebruiker (A) wordt gebruikt ter verificatie van een digitale handtekening (DigSign) van het bestand (Txt), **MET HET KENMERK DAT** de TTP server, bij ontvangst van het vercijferde bestand ((Txt)SesKey) tevens de dan actuele publieke sleutel (PubKeyA) van de eerste gebruiker (A) vercijfert met behulp van de publieke opslagsleutel (PubStorKey) en die vercijferde publieke sleutel ((PubKeyA)PubStorKey) in het opslagmedium (DB) opslaat.

5. Systeem volgens conclusie 4, **MET HET KENMERK DAT**, periodiek,
de TTP server de in het opslagmedium opgeslagen vercijferde publieke sleutel (PubKeyA) van de eerste gebruiker ontcijfert met de private opslagsleutel (SecStorKey);

de TTP server vervolgens een nieuwe versie van het derde sleutelpaar genereert, omvattende een nieuwe publieke opslagsleutel (PubStorKey') en een nieuwe private opslagsleutel (SecStorKey');

de TTP server de ontcijferde publieke sleutel (PubKeyA) van de eerste gebruiker vercijfert met de nieuwe publieke opslagsleutel (PubStorKey') en die aldus vercijferde publieke sleutel ((PubKeyA)PubStorKey') in het opslagmedium opslaat.

6. Systeem volgens conclusie 4, **MET HET KENMERK DAT** de publieke sleutel (PubKeyA) van de eerste gebruiker uit het opslagmedium wordt herwonnen door ontcijfering, met de private opslagsleutel (SecStorKey), van de opgeslagen vercijferde publieke sleutel ((PubKeyA)PubStorKey) van de eerste gebruiker,

dat die aldus herwonnen oorspronkelijke publieke sleutel (PubKeyA) vervolgens wordt vercijferd met de actuele publieke sleutel (PubKeyA' resp. PubKeyB') van de eerste resp. tweede gebruiker (A resp. B) en via het transmissiekanaal naar de eerste resp. tweede gebruiker wordt overgedragen, waarbij de gebruiker, na ontvangst van die vercijferde publieke sleutel ((PubKeyA)PubKeyA' resp. (PubKeyA)PubKeyB') de oorspronkelijk publieke sleutel (PubKeyA) van de eerste gebruiker daaruit kan herwinnen door ontcijfering met zijn actuele private sleutel (SecKeyA' resp. SecKeyB'), en vervolgens de digitale handtekening (DigSign) van het bestand (Txt) kan verifiëren met behulp van de aldus herwonnen oorspronkelijke publieke sleutel (PubKeyA) van de eerste gebruiker.

7. Systeem volgens conclusie 6, **MET HET KENMERK DAT** de digitale handtekening (DigSign) wordt vercijferd met de actuele publieke sleutel (PubKeyA' resp. PublKeyB') van de eerste resp. tweede gebruiker (A resp. B) en naar die eerste resp. tweede gebruiker wordt overgezonden, waarna de ontvangende gebruiker de digitale handtekening herwint door ontcijfering van de ontvangen vercijferde digitale handtekening ((DigSign)PubKeyA' resp. (DigSign)PubKeyB') met zijn private sleutel (SecKeyA' resp. SecKeyB').

8. Systeem volgens conclusie 1, **MET HET KENMERK DAT** de TTP server, bij ontvangst van het vercijferde bestand ((Txt)SesKey) een tijdcode (TStamp) genereert en, gelinkt aan het opgeslagen bestand en vercijferd met de publieke opslagsleutel (PubStorKey), in het opslagmedium (DB) opslaat.

9. Systeem volgens conclusie 8, **MET HET KENMERK DAT**, bij opvraging van het opgeslagen bestand door de eerste of tweede gebruiker (A resp. B), de vercijferde tijdcode ((TStamp)PubStorKey) wordt herwonnen door ontcijfering met de private opslagsleutel (SecStorKey), de herwonnen tijdcode vervolgens vercijferd wordt met de voor de opvragende gebruiker actuele publieke sleutel (PubKeyA' resp. PubKeyB') en naar die gebruiker wordt overgedragen, waarna de gebruiker de vercijferde tijdcode ((TStamp)PubKeyA' resp. (TStamp)PubKeyB') kan ontcijferen met de voor die gebruiker actuele private sleutel (SecKeyA' resp. SecKeyB').

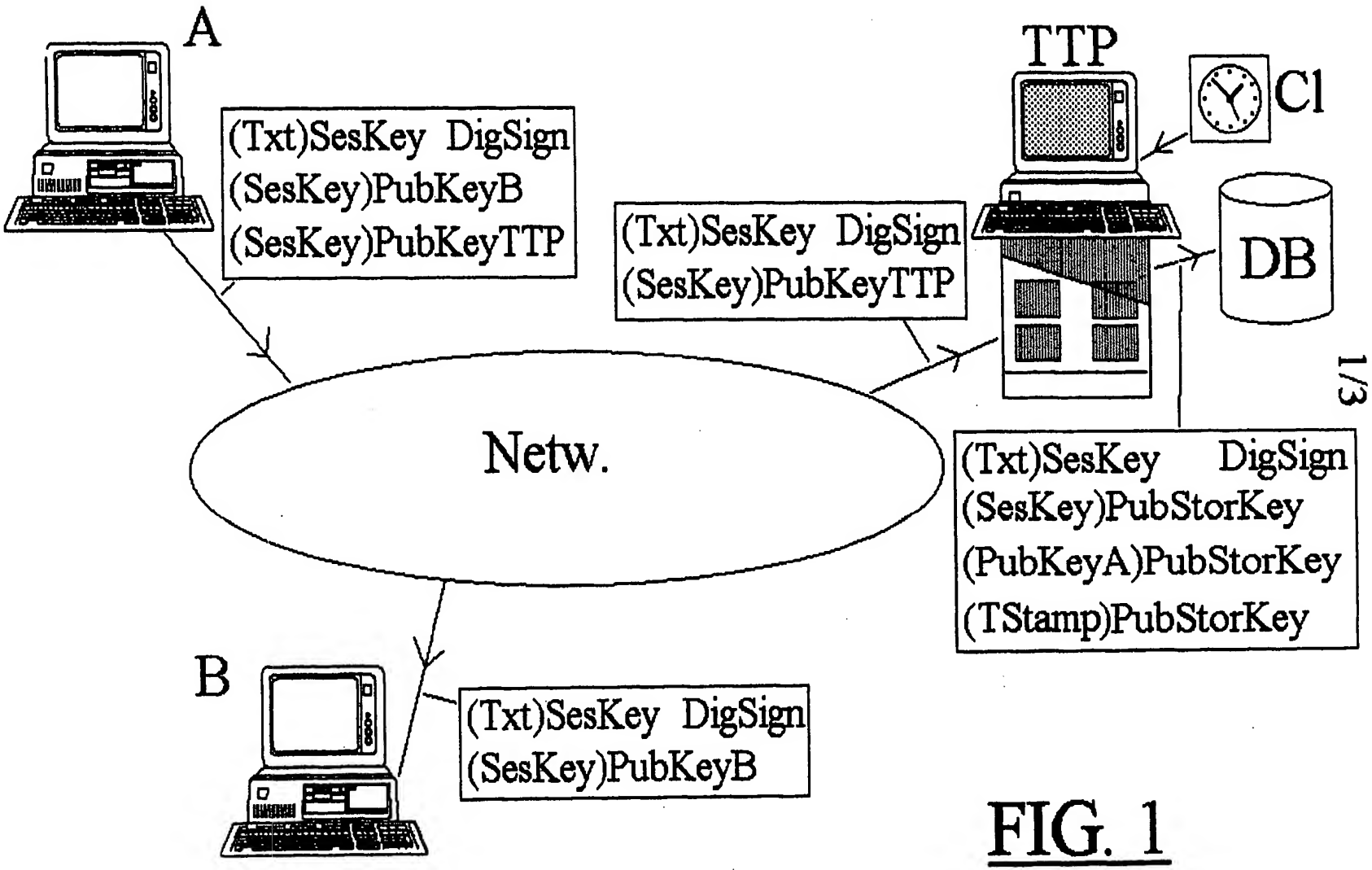

FIG. 1

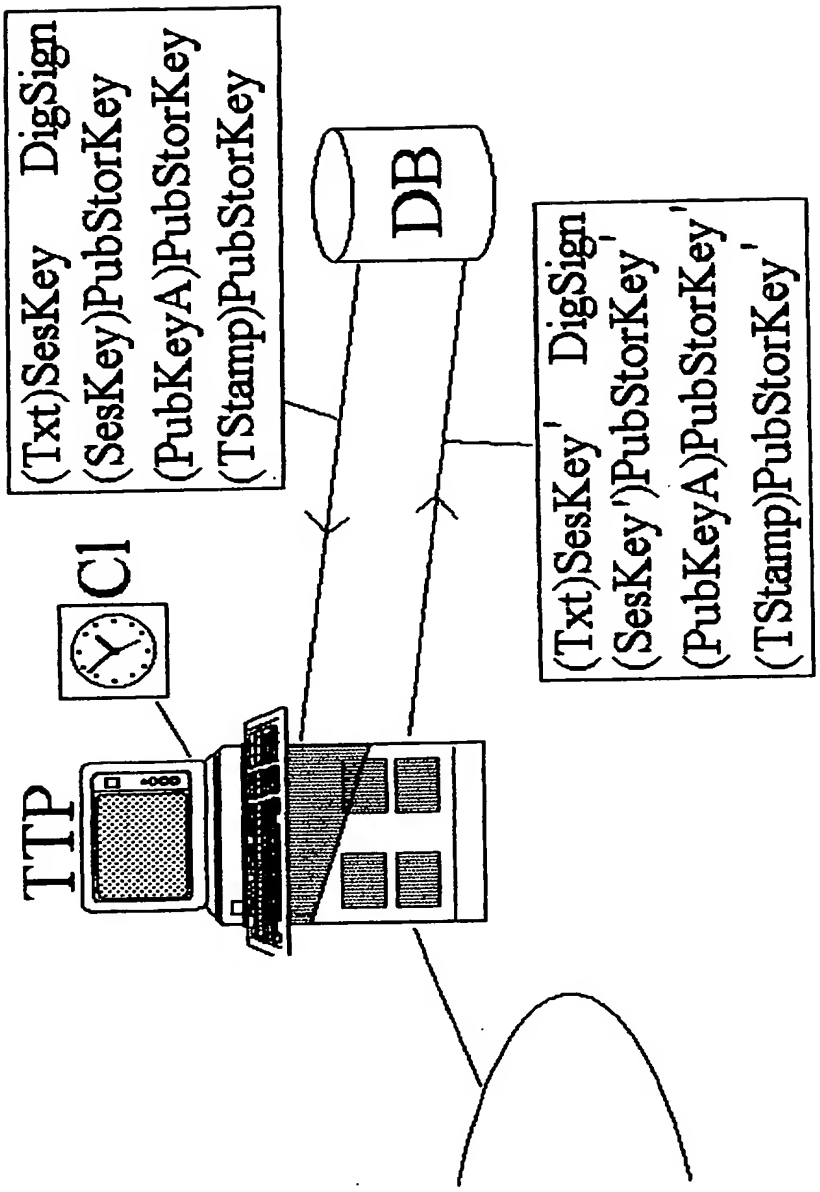
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
DB
(Txt)SesKey' DigSign
(SesKey')PubStorKey'
(PubKeyA)PubStorKey'
(TStamp)PubStorKey'
C1
TTP

FIG. 2

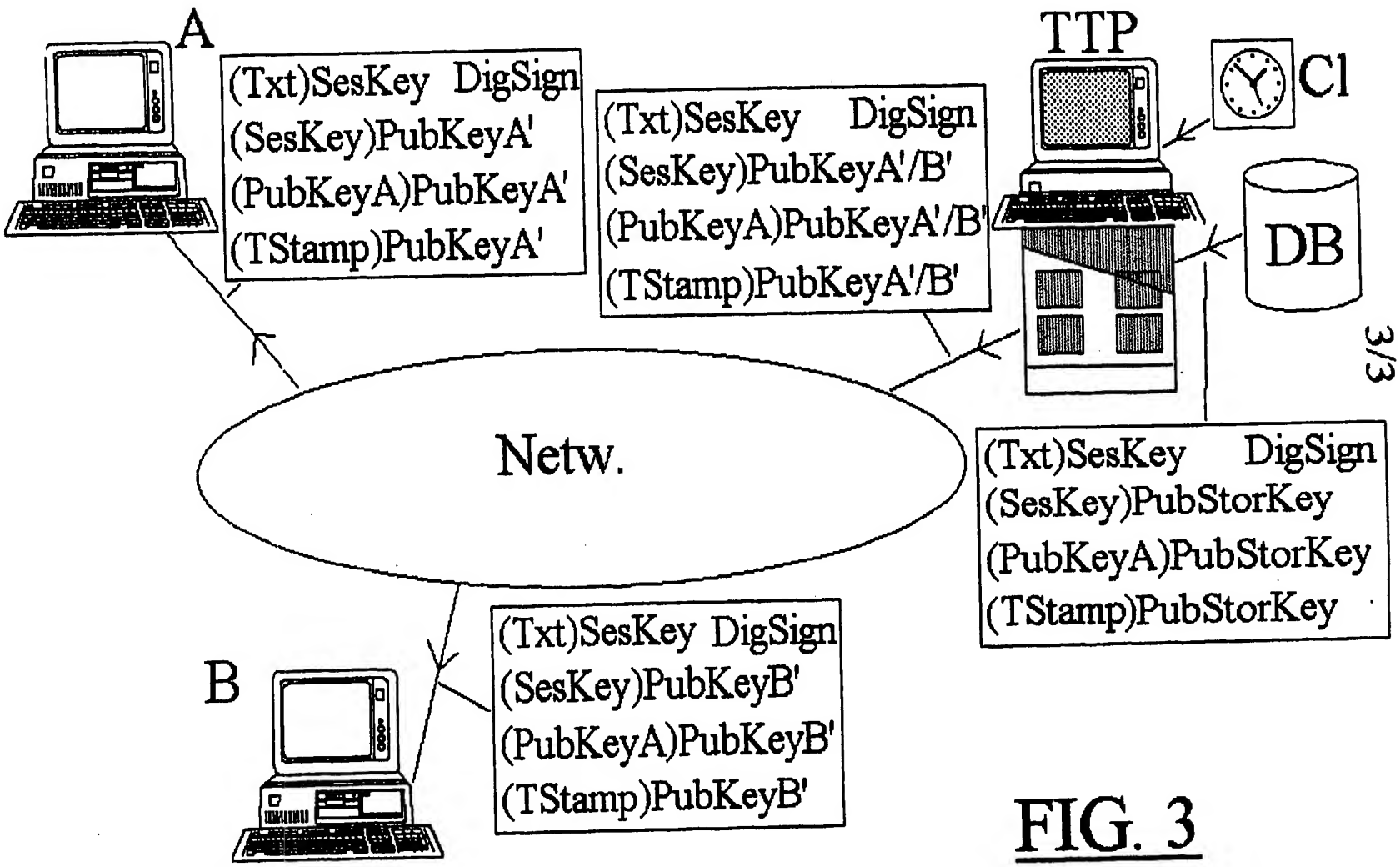
A
(Txt)SesKey DigSign
(SesKey)PubKeyA'
(PubKeyA)PubKeyA'
(TStamp)PubKeyA'
TTP
Cl
(Txt)SesKey DigSign
(SesKey)PubKeyA'/B'
(PubKeyA)PubKeyA'/B'
(TStamp)PubKeyA'/B'
DB
Netw.
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
B
(Txt)SesKey DigSign
(SesKey)PubKeyB'
(PubKeyA)PubKeyB'
(TStamp)PubKeyB'

FIG. 3

KINGDOM OF THE (crest) NETHERLANDS

PATENT OFFICE

This certifies that in the Netherlands, on 25 June 1999, a patent application was filed under number 1012435, in the name of:

Koninklijke KPN N.V.

of Groningen

for: "System for protected storage and management in a TTP server."

and that the documents attached hereto are in accordance with the documents originally submitted

Rijswijk, 29 May 2000

On behalf of the Chairman of the Patent Office,

(signature)

(P.J.C. van den Nieuwenhuijsen

ABSTRACT

System for protected storage in a TTP server. A file (Txt) is transmitted from a first (A) to a second user (B) after being enciphered with a session key (SesKey), which is enciphered with the public key (PubKeyB) of the second user. The session key (SesKey) is also enciphered by the first user with the public key (PubKeyTTP) of the TTP server which, after having received it, deciphers said session key with his private key (SecKeyTTP). The TTP server subsequently enciphers the session key (SesKey) and the (original) public key (PubKeyA) of the first user (A) with a "public" storage key (PubStorKey). The enciphered session key ((SesKey)PubStorKey) and public key ((PubKeyA)PubStorKey) of the first user are stored, together with the enciphered file ((Txt)SesKey), in a storage medium (DB). They are recoverable by the TTP, by deciphering with the private storage key (SecStorKey), and may be transmitted after having been enciphered with the current public keys (PubKeyA' or PubKeyB', as the case may be) of the users.

(FIG. 1)

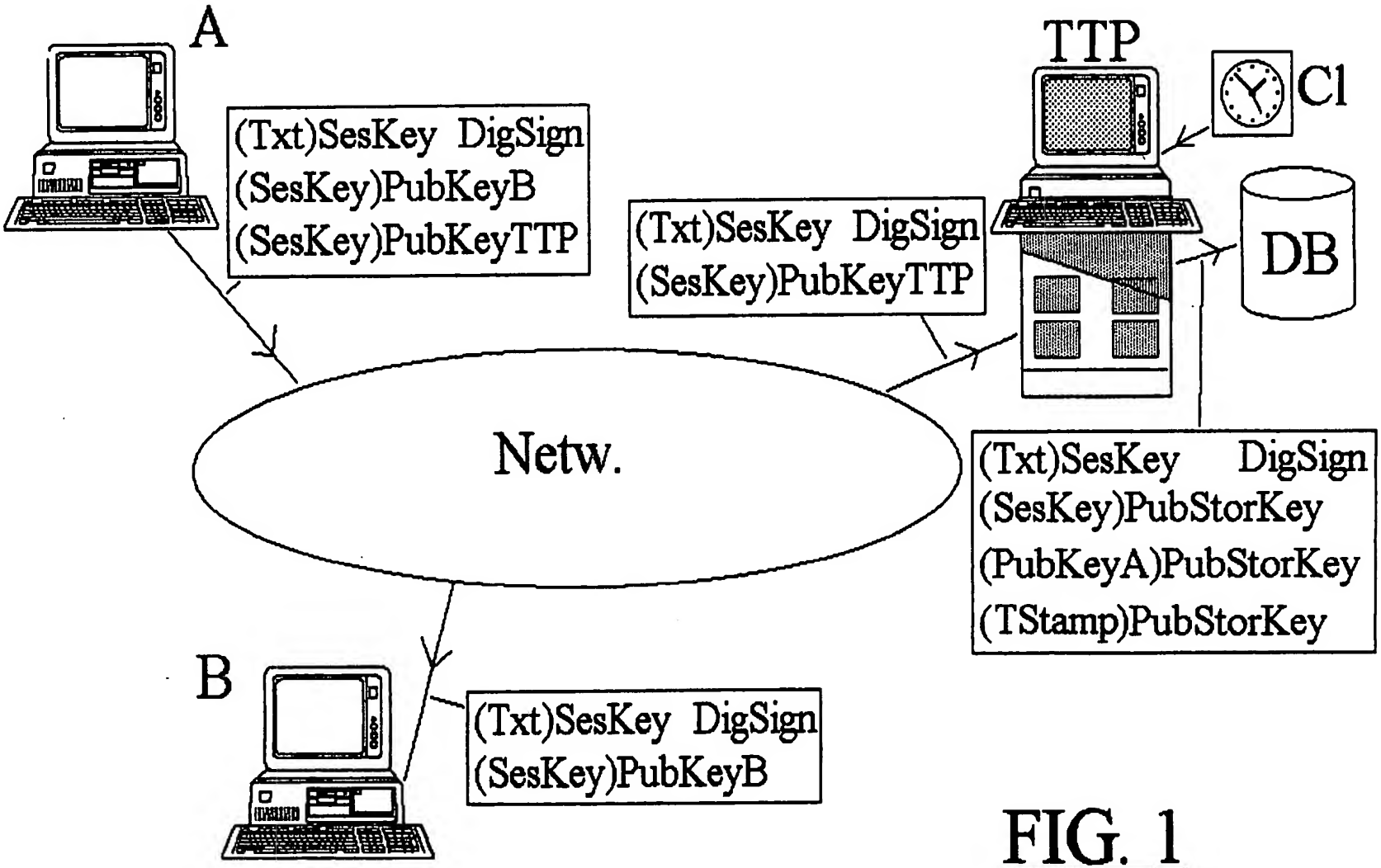

FIG. 1

System for protected storage and management in a TTP server.

BACKGROUND OF THE INVENTION

The invention relates to a system for protected storage and management in a TTP server [TTP = Trusted Third Party] of copies of digital files transmitted, by way of a transmission channel, from a first to a second user.

The invention relates to, in other words, a timeless key and storage system for the benefit of the long-term storage of electronically exchanged (digitally protected) information and protectedly making available (secure retrieving) the stored data.

The few known systems have the following drawbacks:

1) Current protection techniques have a restricted hackability duration guarantee.
2) Limited protection guarantees prior to, during and after long-term storage.
3) Much storage space and effort are required for key management.
4) Protected long-term storage and the associated key and storage management is now either not regulated or very complex in setup.
5) Due to the ever changing software and hardware, it is very difficult to guarantee electronic timelessness.

B. SUMMARY OF THE INVENTION

The object of the invention is to overcome said drawbacks. For this purpose, the invention provides for a system having means for carrying out the functionalities: "Secure Archiving", "Re-encryption" and "Secure Retrieval", which will be discussed below. In this connection, the optional items "Digital Sign" and "Time Stamp" will be discussed separately.

"Secure Archiving"

If, according to the current state of the art, a file is transmitted from a first user to a second user in a safe way, the file is enciphered with a symmetrical session key, which in its turn is enciphered with the public key of the second user. Said second user may decipher the session key with his private key and decipher the file itself with the session key deciphered in this manner.

According to the invention, the session key is also enciphered by the first user with the public key of an "in-line" TTP server (i.e., included in the transmission channel between the first and second users), which TTP server deciphers the session key received with his private key. Thereafter, the TTP server enciphers the deciphered session key with a "public" storage key. The session key enciphered with said public storage key and the file enciphered with the session key are subsequently stored in a storage medium of the TTP.

It should be noted that above and below there is spoken of public and private keys. These are generally known. In general, a public and a private key constitute an asymmetric pair of keys. If a file or a code is enciphered with the public key of an asymmetric pair of keys, said file or code may be deciphered only with the help of the associated private key and vice versa. In general, the public keys are available to "the public", e.g., by way of a publicly accessible data base, such as www.pgp.com. In the present application, it is assumed that the users and the TTP each dispose of a pair of keys, each consisting of a public and a private key, and in particular intented for protecting the mutual data exchange of the files and codes. In addition, the TTP disposes of a pair of keys which is used within the TTP only; the "public" and private keys serve as protected storage or recovery ("secure retrieval"), as the case may be, of files and codes. The public storage key is not, as is normally the case for public keys, put at the disposal of the public.

"Re-encryption"

By way of "periodic maintenance" - from security considerations - the TTP server may at regular points in time store the file once again in the storage medium. For this purpose, the session key with which the file was enciphered is first recovered by deciphering - with the private storage key - the stored (enciphered) session key. Subsequently, the enciphered file stored in the storage medium is deciphered with the recovered session key.

The TTP server then generates a new asymmetric pair of storage keys, consisting of a new public storage key (which is not made available outside the TTP) and a new private storage key, and a new version of the symmetrical session key, whereafter

the TTP enciphers the deciphered file with the new session key and stores it in the storage medium.

The TTP also enciphers the new session key with the new public storage key and stores said enciphered session key in the storage medium.

"Secure Retrieval"

For protected recovery of the stored file, and transmission thereof to the first and/or second user, the symmetrical session key is recovered from the storage medium by deciphering, with the private storage key, the stored enciphered session key. The recovered session key is subsequently enciphered with the current public key of the first or second user, as the case may be, and transmitted to said user by way of the transmission channel, together with a copy of the file stored in the storage medium, enciphered with the session key. After having received the enciphered session key, the user may recover the session key therefrom by deciphering with his private key. Subsequently, the user may decipher the file enciphered with the session key using the recovered session key.

"Digital Sign"

The public key of the first user may - as is well-known - be used to verify a digital signature of the file. A problem arises if - which frequently occurs - the first user at a certain point in time, after the file has been stored in the TTP server, generates a new pair of keys (comprising a public and a private key) and discontinues the old one. For this reason, it is of importance to store the (original) public key of the first user in the TTP server, since only said original key may be used for verifying the digital signature of the stored, later retrievable file.

For this case, the TTP server, after having received the enciphered file, also enciphers the - at that point in time publicly available - public key of the first user, with the public storage key, and stores said enciphered public key in the storage medium.

Periodically, the TTP server — as "periodical maintenance" — deciphers the enciphered (original) public key, stored in the storage medium, of the first user having the private storage key,

and enciphers the deciphered public key of the first user having the newly generated public storage key, and stores said freshly enciphered key in the storage medium.

The public key of the first user may -- upon retrieving the stored file -- be recovered from the storage medium by deciphering, with the private storage key, said stored key. The public key of the first user recovered in this manner is subsequently enciphered with the -- at that point in time publicly available -- public key of the retrieving first or second user, and transmitted by way of the transmission channel. After having received said enciphered public key, the user may recover the original public key of the first user by deciphering his current private key; subsequently, the digital signature of the recovered file may be verified using the recovered original public key of the first user.

"Time Stamp"

If so desired, the TTP server, after the enciphered file has been received and stored, may generate a time stamp and store it, linked to the stored file and enciphered with the public storage key, in the storage medium. In the event of retrieving the stored file by the first or second user, the time stamp is deciphered and subsequently enciphered with the public key valid for said user and transmitted to the user. The user may decipher the enciphered time stamp with his current private key.

DESCRIPTION OF THE FIGURES

Below, the invention is illustrated in further detail by reference to several figures. Figures 1, 2 and 3 illustrate the functions "Secure Archiving", "Re-encryption" and "Secure Retrieval", including the items "Digital Sign" and the "Time Stamp".

FIG. 1: "Secure Archiving"

A file **Txt** is transmitted from a first user **A** to a second user **B** after having been enciphered with a symmetical session key **SesKey**. Said session key is enciphered with the public key **PubKeyB** of the second user. The latter may decipher the session key with his private key **SecKeyB** and the file itself with the deciphered session key.

The session key is also enciphered by the first user with the public key of the TTP server **PubKeyTTP**, which, after having received it, deciphers said session key with his private key **SecKeyTTP**. Thereafter the TTP server enciphers the deciphered session key with a "public" storage key **PubStorKey** of the TTP.

The (transmission) keys of the users A and B each form an asymmetrical pair of keys, **KeyPairA** and **KeyPairB**, respectively, consisting of **PubKeyA** and **SecKeyA**, and **PubKeyB** and **SecKeyB**, respectively. The TTP uses the pair of keys **KeyPairTTP**, consisting of **PubKeyTTP** and **SecKeyTTP**. Finally, for the protected storage of an asymmetrical pair of keys **StorKeyPair**, consisting of the keys **PubStorKey** and **SecStorKey**; contrary to the preceding public keys, **PubStorKey** nor **SecStorKey** is publicly available, but is used exclusively within the TTP.

The session key **(SesKey)PubStorKey** enciphered with the public storage key **PubStorKey** and the file **(Txt)SesKey** enciphered with the session key **SesKey** are subsequently stored in the storage medium **DB** of the TTP.

"Digital Sign"

The public key **PubKeyA** of the first user **A** may be used to verify a digital signature **DigSign** of the file **Txt**. In this case, the TTP server, after having received the enciphered file **(Txt)SesKey**, also enciphers the - at that point in time publicly available - public key **PubKeyA** from the first user **A**, with the public storage key **PubStorKey**, and stores said enciphered public key **(PubKeyA)PubStorKey** in the storage medium **DB**.

"Time Stamp"

After having received and stored the enciphered file **(Txt)SesKey**, the TTP server may generate a time stamp **TStamp** and store it, after enciphering with the public storage key **PubStorKey** and linked to the stored file, in the storage medium **DB** as **(TStamp)PubStorKey**.

FIG. 2: "Re-encryption"

As "periodical maintenance", the TTP server deciphers the enciphered file **(Txt)SesKey** stored in the storage medium with the session key **SesKey**, which for that purpose is recovered by deciphering the stored session key **(SesKey)PubStorKey** with the

private storage key **SecStorKey**. The TTP server subsequently generates a fresh pair of storage keys **StorKeyPair**, comprising a new "public" storage key **PubStorKey'** and a new private storage key **SecStorKey'**, as well as a new version of the symmetrical session key **SesKey'**. The TTP subsequently enciphers the deciphered file **Txt** with the new session key **SesKey'** and stores the file **(Txt)SesKey'** enciphered in this manner in the storage medium **DB**.

The TTP also enciphers the new session key with the new public storage key **PubStorKey'** and stores the session key **(SesKey')PubStorKey'** enciphered in this manner in the storage medium **DB**.

"Digital Sign"

During the periodical maintenance, the TTP server also deciphers the enciphered public key **(PubKeyA)PubStorKey** stored in the storage medium of the first user with the private storage key **SecStorKey**, and subsequently enciphers the deciphered public key **PubKeyA** with the newly generated public storage key **PubStorKey'** and stores the public key **(PubKeyA)PubStorKey'** enciphered in this manner in the storage medium.

"Time Stamp"

During the periodical maintenance, the TTP server also deciphers the enciphered time stamp **(TStamp)PubStorKey** stored in the storage medium with the private storage key **SecStorKey**, and subsequently enciphers the deciphered time stamp with the newly generated public storage key **PubStorKey'** and stores the time stamp **(TStamp)PubStorKey'** enciphered in this manner in the storage medium.

FIG. 3: "Secure Retrieval"

For protected recovery of the file **Txt**, and the transmission thereof to the first and second users **A** and **B**, respectively, the symmetrical session key **SesKey** is recovered from the storage medium by deciphering, with the private storage key **SecStorKey**, the stored enciphered session key **(SesKey)PubStorKey**. The recovered session key **SesKey** is subsequently enciphered with the then current public key **PubKeyA`** or **PubKeyB`**, as the case may be, from the querying first or

second user **A** or **B**, as the case may be, and transmitted to said user by way of the transmission channel, together with a copy of the file stored in the storage medium, with the user, after having received the enciphered session key **(SesKey)PubKeyA`** or **(SesKey)PubKeyB`**, being capable of recovering the session key therefrom by deciphering, with his private key **SecKeyA`** or **SecKeyB`**, as the case may be, and subsequently being capable of deciphering the file **(Txt)SesKey** using the recovered session key.

"Digital Sign"

The original public key **PubKeyA** of the first user, necessary for verifying the digital signature of the recovered file, may be recovered from the storage medium by deciphering, with the private storage key **SecStorKey**, the stored public key **(PubKeyA)PubStorKey** of the first user enciphered with the public storage key. The deciphered public key **PubKeyA** of the first user recovered in this manner is subsequently enciphered with the current public key **PubKeyA`** or **PubKeyB`**, as the case may be, of the retrieving first or second user **A** or **B**, as the case may be, and transmitted to the user by way of the transmission channel. After having received said enciphered public key **(PubKeyA)PubKeyA`** or **(PubKeyA)PubKeyB`**, as the case may be, the user may recover the original public key **PubKeyA** of the first user therefrom by deciphering, with his current private key **SecKeyA`** or **SecKeyB`**, as the case may be. Subsequently, the digital signature **DigSign** of the file **Txt** may be verified using the recovered public key **PubKeyA** of the first user.

It should be noted that it is preferable to - otherwise than is shown in FIG. 3 - not transmit the digital signature **DigSign** unencipheredly to the first or second user, as the case may be, but enciphered with the public key of user **A** or **B**, as the case may be: instead of **"DigSign"**, the TTP server then transmits **"(DigSign)PubKeyA`"** or **"(DigSign)PubKeyB`"**, as the case may be. At the user's side, the digital signature may be recovered by deciphering, with the private keys of **A** and **B**, **SecKeyA** and **SecKeyB**, respectively.

"Time Stamp"

When the stored file is retrieved by the first or second user, the time stamp is first retrieved by deciphering

(TStamp)PubStorKey with the private storage key **SecStorKey**. The recovered time stamp is subsequently enciphered with the user's current public key **PubKeyA'** or **PubKeyB'**, as the case may be, and transmitted to said user. Thereafter, the user may decipher the enciphered time stamp **(TStamp)PubKeyA'** or **(TStamp)PubKeyB'**, as the case may be, with his current private key **SecKeyA'** or **SecKeyB'**, as the case may be.

CLAIMS

1. System for protectedly storing and managing, in a TTP server, copies of digital files which are transmitted, by way of a transmission channel, from a first to a second user, characterised in that

- a file (Txt) is transmitted from the first user (A) to a second user (B) after having been enciphered with a symmetrical session key (SesKey), which session key is enciphered using the public key (PubKeyB) of a first asymmetrical pair of keys (KeyPairB) associated with the second user, which second user, after having received it, may decipher the session key using the private key (SecKeyB) of said first asymmetrical pair of keys (KeyPairB) and subsequently may decipher the file using the session key deciphered in this manner, the session key (SesKey) also being enciphered by the first user (A) using the public key (PubKeyTTP) of a second asymmetrical pair of keys (KeyPairTTP) associated with the TTP server, which TTP server, after having received it, deciphers said session key using the private key (SecKeyTTP) from said second asymmetrical pair of keys (KeyPairTTP), whereafter the TTP server enciphers the deciphered session key (SesKey) using the public key of a third asymmetrical pair of keys (StorKeyPair), hereinafter to be referred to as public storage key (PubStorKey), and stores the session key ((SesKey)PubStorKey) enciphered with said storage key, together with the file ((Txt)SesKey) enciphered with the session key (SesKey), in a storage medium (DB).

2. System according to claim 1, characterised in that, periodically,

- the TTP server deciphers the enciphered file ((Txt)SesKey) stored in the storage medium with the session key (SesKey), which for that purpose is recovered in advance by deciphering the stored enciphered session key ((SesKey)PubStorKey) with the private key of the third pair of keys (StorKeyPair), hereinafter to be referred to as the private storage key (SecStorKey);

- the TTP server subsequently generates a new version of the third pair of keys, comprising a new public storage key (PubStorKey') and a new private storage key (SecStorKey'), and a new version of the symmetrical session key (SesKey'), whereafter the TTP enciphers the deciphered file (Txt) with the new session key (SesKey') and stores the file ((Txt)SesKey') enciphered in this manner in the storage medium (DB);
- the TTP server enciphers the new session key (SesKey') with the new public storage key (PubStorKey') and stores the session key ((SesKey')PubStorKey') enciphered in this manner in the storage medium (DB).

3. System according to claim 1, characterised in that, for protected recovery of the file (Txt) and transmission thereof to the first user (A) or the second user (B), as the case may be, the symmetrical session key (SesKey) is recovered from the storage medium by deciphering, with the private storage key (SecStorKey), the stored enciphered session key ((SesKey)PubStorKey), whereafter the recovered session key (SesKey) is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted to the user by way of the transmission channel, together with a copy of the file ((Txt)SesKey) stored in the storage medium, with the user, after having received the enciphered session key ((SesKey)PubKeyA' or (SesKey)PubKeyB', as the case may be), being capable of recovering the session key therefrom by deciphering using the user's private key (SecKeyA' or SecKeyB', as the case may be), and subsequently being capable of deciphering the enciphered file ((Txt)SesKey) using the recovered session key.

4. System according to claim 1, the public key (PubKeyA) of the first user (A) being used to verify a digital signature (DigSign) of the file (Txt), characterised in that the TTP server, after having received the enciphered file ((Txt)SesKey), also enciphers the then current public key (PubKeyA) of the first user (A) using the public storage key (PubStorKey), and stores said enciphered public key ((PubKeyA)PubStorKey) in the storage medium (DB).

5. System according to claim 4, characterised in that, periodically,

- the TTP server deciphers the enciphered public key (PubKeyA) of the first user stored in the storage medium with the private storage key (SecStorKey);
- the TTP server subsequently generates a new version of the third pair of keys, comprising a new public storage key (PubStorKey') and a new private storage key (SecStorKey');
- the TTP server enciphers the deciphered public key (PubKeyA) of the first user with the new public storage key (PubStorKey') and stores said public key ((PubKeyA)PubStorKey'), enciphered in this manner, in the storage medium.

6. System according to claim 4, characterised in that the public key (PubKeyA) of the first user is recovered from the storage medium by deciphering, with the private storage key (SecStorKey), the stored enciphered public key ((PubKeyA)PubStorKey) of the first user, that said original public key (PubKeyA) recovered in this manner is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted by way of the transmission channel to the first or second user, as the case may be, with the user, after having received said enciphered public key ((PubKeyA)PubKeyA' or (PubKeyA)PubKeyB', as the case may be) being capable of recovering the original public key (PubKeyA) of the first user therefrom by deciphering with his current private key (SecKeyA' or SecKeyB', as the case may be), and subsequently being capable of verifying the digital signature (DigSign) of the file (Txt) using the original public key (PubKeyA) of the first user recovered in this manner.

7. System according to claim 6, characterised in that the digital signature (DigSign) is enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) of the first or second user (A or B, as the case may be), and is transmitted to said first or second user, as the case may be, whereafter the receiving user recovers the digital signature by deciphering the

received, enciphered digital signature ((DigSign)PubKeyA' or (DigSign)PubKeyB', as the case may be) with his private key (SecKeyA' or SecKeyB', as the case may be).

8. System according to claim 1, characterised in that the TTP server, after having received the enciphered file ((Txt)SesKey) generates a time stamp (TStamp) and stores it, linked to the stored file and enciphered with the public storage key (PubStorKey), in the storage medium (DB).

9. System according to claim 8, characterised in that, in the event of retrieving the stored file by the first or second user (A or B, as the case may be) the enciphered time stamp ((TStamp)PubStorKey) is recovered by deciphering with the private storage key (SecStorKey), the recovered time stamp is subsequently enciphered with the current public key (PubKeyA' or PubKeyB', as the case may be) for the querying user, and is transmitted to said user, whereafter the user may decipher the enciphered time stamp ((TStamp)PubKeyA' or (TStamp)PubKeyB', as the case may be) with the private key (SecKeyA' or SecKeyB', as the case may be) current for said user.

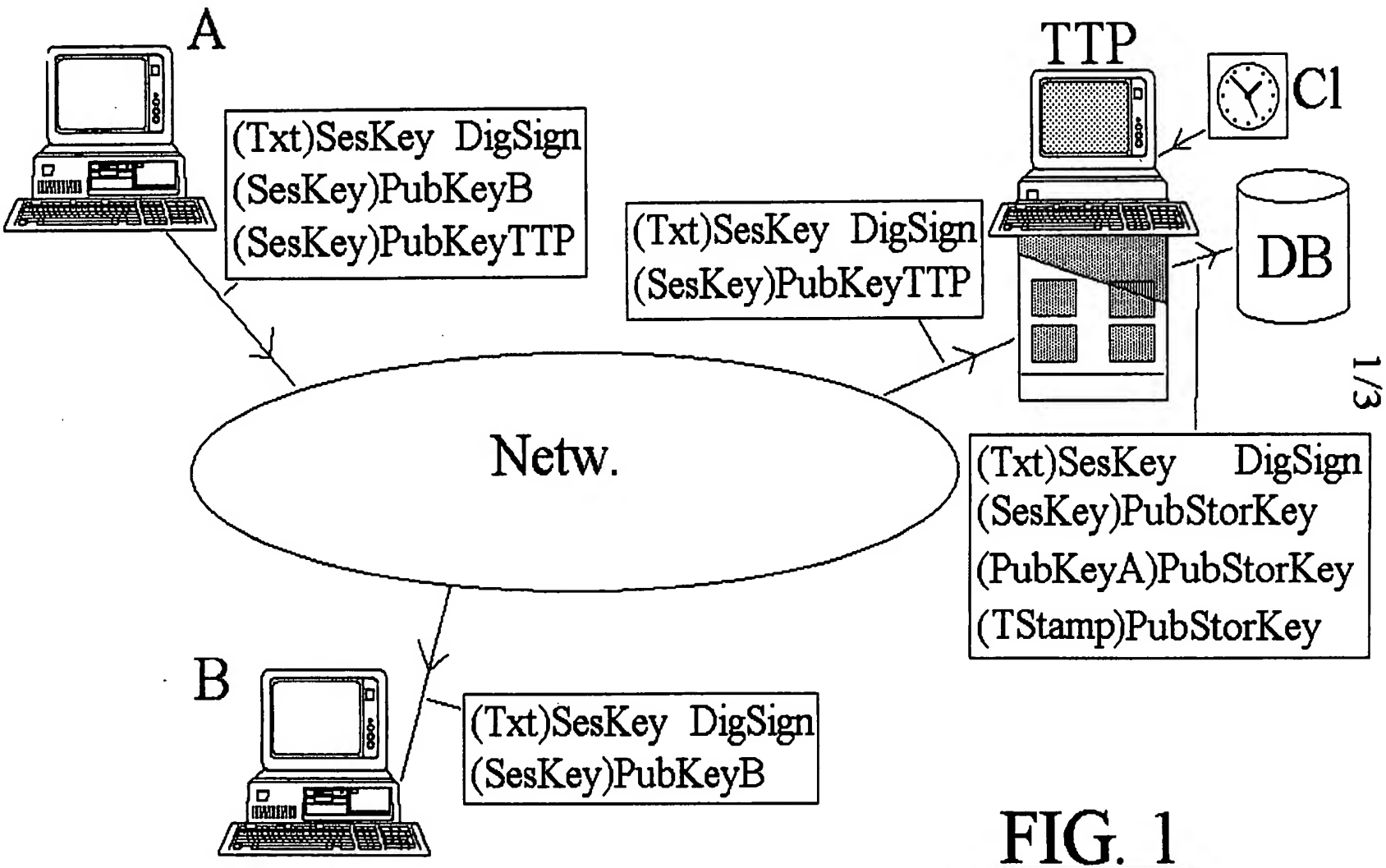

FIG. 1

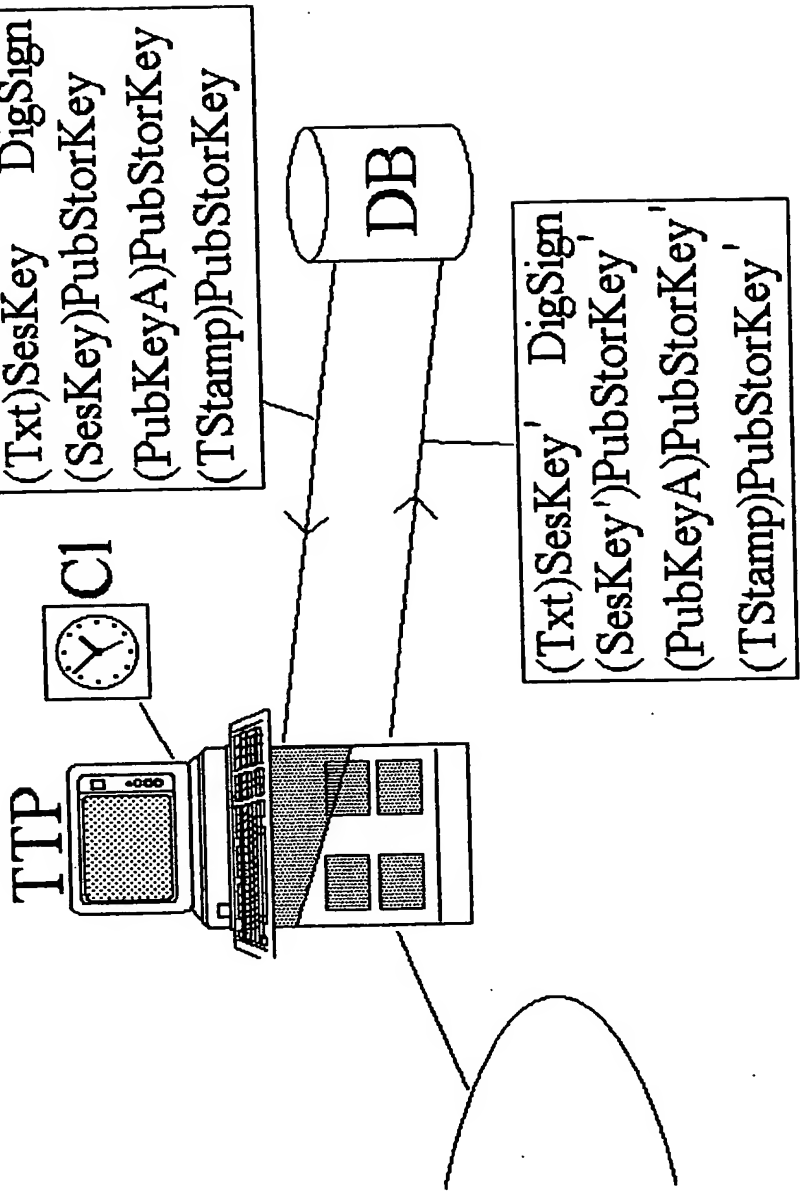
(Txt)SesKey DigSign
(SesKey)PubStorKey
(PubKeyA)PubStorKey
(TStamp)PubStorKey
DB
(Txt)SesKey' DigSign'
(SesKey')PubStorKey'
(PubKeyA)PubStorKey'
(TStamp)PubStorKey'
Cl
TTP

FIG. 2

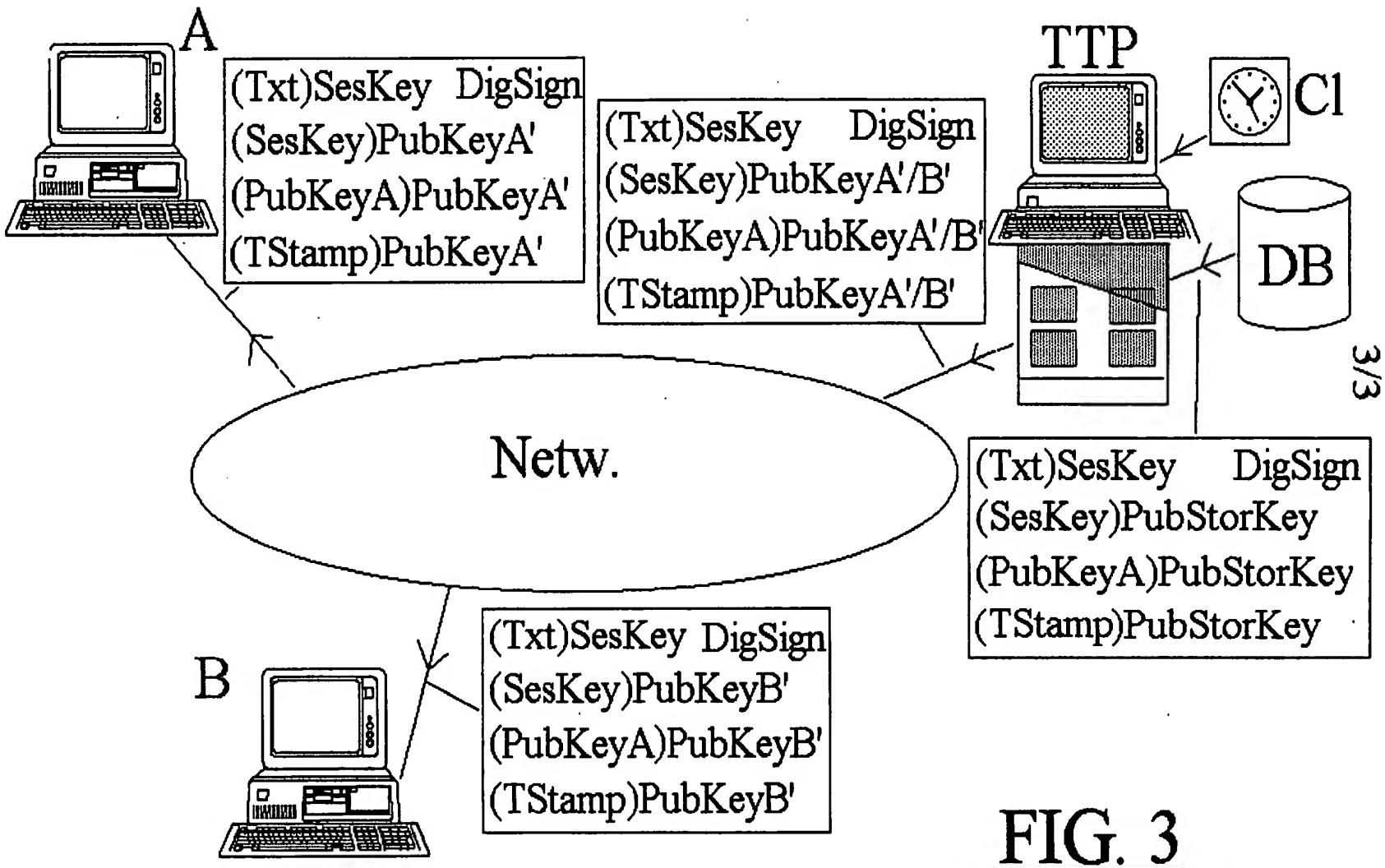

FIG. 3